AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer n that is a product of two large prime numbers p and q, and of a public exponent e, said algorithm also including a private key, said method determining a set E comprising a predetermined number of prime numbers e_i that can correspond to the value of the public exponent e, and comprising the following steps:

a) computing a value $\Phi = \prod_{ei \in E} ei$

such that Φ / e_i is less than $\Phi(n)$ for any e_i belonging to E, where Φ is the Euler totient function;

b) applying the value Φ to a predetermined computation involving, as a modular product, only the modular product of Φ multiplied by said private key of the algorithm;

c) for each e_i, testing whether the result of said predetermined computation is equal to a value Φ / e_i:

- if so, then attributing the value e_i to e, and storing e ~~for subsequent use in computations of said cryptography algorithm~~;

- otherwise, indicating that the computations of the cryptography algorithm using the value e cannot be performed; and

d) performing a cryptographic operation on data using the stored value for e.

2. (Previously Presented) A method according to claim 1, wherein the cryptography algorithm is based on an RSA-type algorithm in standard mode.

3. (Previously Presented) A method according to claim 2, wherein the predetermined computation of step b) comprises computing a value C:

C = Φ .d modulo Φ(n), where d is the corresponding private key of the RSA algorithm such that e.d = 1 modulo Φ(n) and Φ is the Euler totient function.

4. (Previously Presented) A method according to claim 2, wherein the predetermined computation of step b) comprises computing a value C:

C = Φ .d modulo Φ (n), where d is the corresponding private key of the RSA algorithm such that e.d = 1 modulo Φ (n), with Φ being the Carmichael function.

5. (Previously Presented) A method according to claim 1, wherein the cryptography algorithm is based on an RSA-type algorithm in CRT mode.

6. (Previously Presented) A method according to claim 5, wherein the predetermined computation of step b) comprises computing a value C:

C = Φ .d_p modulo (p-1), where d_p is the corresponding private key of the RSA algorithm such that e.d_p = 1 modulo (p-1).

7. (Previously Presented) A method according to claim 5, wherein the predetermined computation of step b) comprises computing a value C:

C = Φ .d_q modulo (q-1), where d_q is the corresponding private key of the RSA algorithm such that e.d_q = 1 modulo (q-1).

8. (Previously Presented) A method according to claim 5, wherein the predetermined computation of step b) comprises computing two values C_1 and C_2 such that:

C_1 = Φ .d_p modulo (p-1), where d_p is the corresponding private key of the RSA algorithm such that e.d_p = 1 modulo (p-1);

C_2 = Φ .d_q modulo (q-1), where d_q is the corresponding private key of the RSA algorithm such that e.d_q = 1 modulo (q-1);

and wherein the test step c) comprises, for each e_i, testing whether C_1 and/or C_2 is equal to the value Φ /e_i:

- if so, then attributing the value e_i to e and storing e for subsequent use in computations of said cryptography algorithm;

- otherwise, indicating that the computations of said cryptography algorithm using the value e cannot be performed.

9. (Previously Presented) A method according to claim 3 and in which a value e_i has been attributed to e, wherein the computations using the value e comprise:

choosing a random integer r;

computing a value d* such that $d^* = d+r.(e.d-1)$; and

implementing a private operation of the algorithm in which a value x is obtained from a value y by applying the relationship $x = y^{d^*}$ modulo n.

10. (Previously Presented) A method according to claim 2, in which a value e_i has been attributed to e, and further including the step, after a private operation of the algorithm, of obtaining a value x from a value y, and wherein the computations using the value e comprise checking whether $x^e = y$ modulo n.

11. (Previously Presented) A method according to claim 5, in which a value e_i has been attributed to e, and further including the step, after a private operation of the algorithm, of obtaining a value x from a value y, and wherein the computations using the value e comprise checking whether $x^e = y$ modulo p and whether $x^e = y$ modulo q.

12. (Previously Presented) A method according to claim 1, wherein the set E comprises at least the following e_i values: 3, 17, $2^{16}+1$.

13. (Currently Amended) An electronic component comprising means for ~~implementing the method according to claim 1~~ executing the following steps:

a) computing a value $\Phi = \prod_{ei \in E} ei$

such that Φ / e_i is less than $\Phi(n)$ for any e_i belonging to E, where Φ is the Euler totient function;

b) applying the value Φ to a predetermined computation involving, as a modular product, only the modular product of Φ multiplied by a private key of the algorithm;

c) for each e_i, testing whether the result of said predetermined computation is equal to a value Φ / e_i:

- if so, then attributing the value e_i to e, and storing e;
- otherwise, indicating that the computations of the cryptography algorithm using the value e cannot be performed; and

d) performing a cryptographic operation on data using the stored value for e.

14. (Previously Presented) A smart card including the electronic component of claim 13.

15. (Currently Amended) A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer n that is a product of two large prime numbers p and q, and of a public exponent e, said method determining a set E comprising a predetermined number of prime numbers e_i that can correspond to the value of the public exponent e, and comprising the following steps:

a) choosing a value e_i from the values of the set E;

b) if $\Phi(p)= \Phi(q)$, where $\Phi(n)$, $\Phi(p)$, and $\Phi(q)$ are functions giving the number of bits encoding respectively the number n, the number p, and the number q, testing whether the chosen e_i value satisfies the relationship:

$(1-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+1}$

or said relationship as simplified:

$(-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+1}$

c) if the test relationship applied in the preceding step is satisfied, defining $e = e_i$, and storing e ~~for subsequent use in computations of said cryptography algorithm~~;

- otherwise, reiterating the preceding steps while choosing another value for e_i from the set E until an e_i value can be attributed to e and, if no e_i value can be attributed to e, then indicating that the computations of said cryptography algorithm using the value of e cannot be performed; and

d) performing a cryptographic operation on data using the stored value for e.

16. (Previously Presented) A method of securely implementing a public-key cryptography algorithm according to claim 15, wherein step b is performed in the following manner when $\Phi(p) \neq \Phi(q)$, i.e. when p and q are unbalanced, testing whether the chosen e_i value satisfies the following relationship:

$(1-e_i.d)$ modulo $n < e_i.2^{g+1}$

or said relationship as simplified:

$(-e_i.d)$ modulo $n < e_i.2^{g+1}$

with $g=\max(\Phi(p), \Phi(q))$, if $\Phi(p)$ and $\Phi(q)$ are known, or, otherwise, with $g=\Phi(n)/2+t$, where t designates the imbalance factor or a limit on that factor.

17. (Previously Presented) A method according to claim 16, wherein, for all values of i, $e_i \leq 2^{16}+1$, step b) is replaced by another test step comprising:

b) if $\Phi(p)=\Phi(q)$, testing whether the chosen e_i value satisfies the relationship:

$(1-e_i.d)$modulo $n < e_i.2^{(\Phi(n)/2)+17}$

or said relationship as simplified:

$(-e_i.d)$modulo $n < e_i.2^{(\Phi(n)/2)+17}$

where $\Phi(p)$, $\Phi(q)$, and $\Phi(n)$ are functions giving the numbers of bits respectively encoding the number p, the number q, and the number n;

otherwise, when p and q are unbalanced, testing whether the chosen e_i value satisfies the following relationship:

$(1-e_i.d)$ modulo $n < e_i.2^{g+17}$

or said relationship as simplified:

$(-e_i.d)$ modulo $n < e_i.2^{g+17}$

with $g=\max(\Phi(p),\Phi(q))$, if $\Phi(p)$ and $\Phi(q)$ are known, or, otherwise, with $g=\Phi(n)/2+t$, where t designates the imbalance factor or a limit on that factor.

18. (Previously Presented) A method according to claim 16, wherein step b) is replaced with another test step comprising:

testing whether the chosen e_i value satisfies the relationship whereby:

a predetermined number of the first most significant bits of $(1-e_i.d)$ modulo n are zero;

or said relationship as simplified whereby:

said predetermined number of the first most significant bits of $(-e_i.d)$ modulo n are zero.

19. (Previously Presented) A method according to claim 18, wherein the test is performed on the first 128 most significant bits.

20. (Previously Presented) A method according to claim 15, wherein the cryptography algorithm is based on an RSA-type algorithm in standard mode.

21. (Previously Presented) A method according to claim 15 wherein, when an e_i value has been attributed to e, the computations using the value e comprise:

- choosing a random integer r;
- computing a value d* such that d* = d+r.(e.d-1);

implementing a private operation of the algorithm in which a value x is obtained from a value y by applying the relationship $x = y^{d^*}$ modulo n.

22. (Previously Presented) A method according to claim 15 wherein, when an e_i value has been attributed to e, after a private operation of the algorithm, a value x is_obtained from a value y and the computations using the value e comprise checking whether $x_e = y$ modulo n.

23. (Previously Presented) A method according to claim 15, wherein the set E comprises at least the following e_i values: 3, 17, $2^{16}+1$.

24. (Previously Presented) A method according to claim 23, wherein the preferred choice of the values e_i from the values of the set E is made in the following order: $2^{16}+1$, 3, 17.

25. (Currently Amended) An electronic component comprising means for ~~implementing the method according to claim 15~~ executing the following steps:

a) choosing a value e_i from the values of the set E;

b) if $\Phi(p)= \Phi(q)$, where $\Phi(n)$, $\Phi(p)$, and $\Phi(q)$ are functions giving the number of bits encoding respectively the number n, the number p, and the number q, where n is an integer that is a product of two large prime numbers p and q, testing whether the chosen e_i value satisfies the relationship:

$(1-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+1}$

or said relationship as simplified:

$(-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+1}$

c) if the test relationship applied in the preceding step is satisfied, defining $e = e_i$, and storing e;

- otherwise, reiterating the preceding steps while choosing another value for e_i from the set E until an e_i value can be attributed to e and, if no e_i value can be attributed to e, then indicating that the computations of said cryptography algorithm using the value of e cannot be performed; and

d) performing a cryptographic operation on data using the stored value for e.

26. (Previously Presented) A smart card including the electronic component of claim 25 .

27. (Previously Presented) A method according to claim 15, wherein, for all values of i, $e_i \leq 2^{16}+1$, step b) is replaced by another test step comprising:

b) if $\Phi(p)=\Phi(q)$, testing whether the chosen e_i value satisfies the relationship:

$(1-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+17}$

or said relationship as simplified:

$(-e_i.d)\text{modulo } n < e_i.2^{(\Phi(n)/2)+17}$

where $\Phi(p)$, $\Phi(q)$, and $\Phi(n)$ are functions giving the numbers of bits respectively encoding the number p, the number q, and the number n;

otherwise, when p and q are unbalanced, testing whether the chosen e_i value satisfies the following relationship:

$(1-e_i.d) \text{ modulo } n < e_i.2^{9+17}$

or said relationship as simplified:

$(-e_i.d)$ modulo n < $e_i.2^{g+17}$

with g=max (Φ(p),Φ(q)), if Φ(p) and Φ(q) are known, or, otherwise, with g=Φ(n)/2+t, where t designates the imbalance factor or a limit on that factor.

28. (Previously Presented) A method according to claim 15, wherein step b) is replaced with another test step comprising:

testing whether the chosen e_i value satisfies the relationship whereby:

a predetermined number of the first most significant bits of $(1-e_i.d)$ modulo n are zero;

or said relationship as simplified whereby:

said predetermined number of the first most significant bits of $(-e_i.d)$ modulo n are zero.

29. (Previously Presented) A method according to claim 4 and in which a value e_i has been attributed to e, wherein the computations using the value ecomprise:

choosing a random integer r;

computing a value d* such that d* = d+r.(e.d-1); and

implementing a private operation of the algorithm in which a value x is obtained from a value y by applying the relationship $x = y^{d^*}$ modulo n.

30. (New) A method according to claim 1, wherein said cryptographic operation comprises at least one of encrypting data, decrypting data, signing a message and authenticating a message.

31. (New) A method according to claim 15, wherein said cryptographic operation comprises at least one of encrypting data, decrypting data, signing a message and authenticating a message.